WO9839745

Publication Title:

PORTABLE DATA CARRIER AND METHOD FOR CRYPTOGRAPHICALLY SECURE USE THEREOF WITH INTERCHANGEABLE KEYS

Abstract:

Abstract of WO 9839745

(A2) Translate this text The invention relates to a portable data carrier, especially a chip card, to store data in the form of data records, wherein cryptographic keys are memorized on the data carrier in order to protect the writing and reading of said data records. A series of keys is thus stored on the data carrier to perform this task. Means are provided to make the keys in the data carrier unfit for use. Also disclosed is a method for using a data carrier wherein the use of each key to read or write data is preceded by verification of whether the key is older than the key whose identification mark is stored on the data carrier. The use of said key is denied if the results of the verification are positive.

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro
INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :
G07F 7/10, H04L 9/00

A2

(11) Internationale Veröffentlichungsnummer: WO 98/39745

(43) Internationales Veröffentlichungsdatum: 11. September 1998 (11.09.98)

(21) Internationales Aktenzeichen: PCT/EP98/01269

(22) Internationales Anmeldedatum: 5. März 1998 (05.03.98)

(30) Prioritätsdaten:
197 09 274.8 6. März 1997 (06.03.97) DE

(71) Anmelder: DEUTSCHE TELEKOM AG [DE/DE]; Friedrich–Ebert–Allee 140, D–53113 Bonn (DE).

(72) Erfinder: HARTLEIF, Siegfried; Heinrich–Heine–Strasse 18A, D–64823 Groß–Umstadt (DE). SCHAEFER–LORINSER, Frank; Potsdamerstrasse 88, D–64372 Ober–Ramstadt (DE).

(81) Bestimmungsstaaten: HU, NO, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

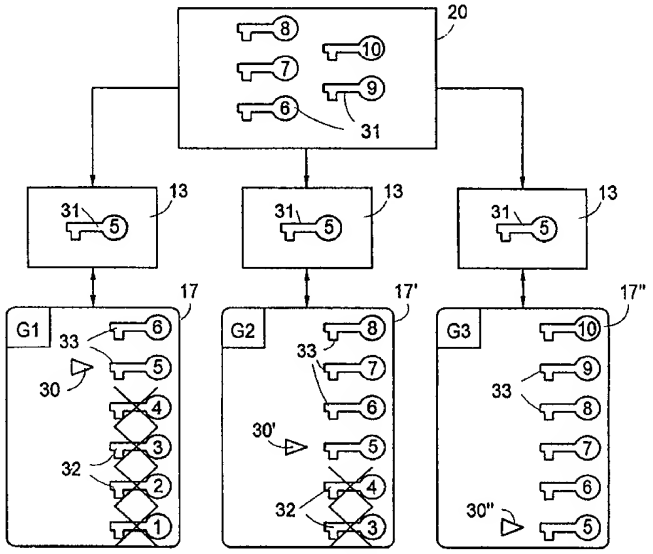
Veröffentlicht
Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.

(54) Title: PORTABLE DATA CARRIER AND METHOD FOR CRYPTOGRAPHICALLY SECURE USE THEREOF WITH INTERCHANGEABLE KEYS

(54) Bezeichnung: TRAGBARER DATENTRÄGER UND VERFAHREN ZU DESSEN KRYPTOGRAPHISCH GESICHERTEN BENUTZUNG MIT AUSTAUSCHBAREN KRYPTOGRAPHISCHEN SCHLÜSSELN

(57) Abstract

The invention relates to a portable data carrier, especially a chip card, to store data in the form of data records, wherein cryptographic keys are memorized on the data carrier in order to protect the writing and reading of said data records. A series of keys is thus stored on the data carrier to perform this task. Means are provided to make the keys in the data carrier unfit for use. Also disclosed is a method for using a data carrier wherein the use of each key to read or write data is preceded by verification of whether the key is older than the key whose identification mark is stored on the data carrier. The use of said key is denied if the results of the verification are positive.



(57) Zusammenfassung

Bei einem tragbaren Datenträger, insbesondere Chipkarte, zum Speichern von Daten in Form von Datensätzen, wobei zur Absicherung des Schreibens und Lesens der Datensätze kryptographische Schlüssel auf dem Datenträger gespeichert sind, ist eine Reihe von Schlüsseln für den jeweiligen Verwendungszweck auf dem Datenträger gespeichert. Es sind Mittel zur Unbrauchbarmachung von Schlüsseln im Datenträger vorgesehen. Es wird ein Verfahren zur Benutzung des Datenträgers angegeben, wobei vor jeder Benutzung eines Schlüssels zum Schreiben oder Lesen von Daten geprüft wird, ob der Schlüssel älter ist als derjenige, dessen Identifikationsmerkmal auf dem Datenträger gespeichert ist. Bei positivem Ergebnis dieser Prüfung wird die Benutzung des Schlüssels abgelehnt.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

Tragbarer Datenträger und Verfahren zu dessen kryptographisch gesicherten Benutzung mit austauschbaren kryptographischen Schlüsseln

Die Erfindung betrifft einen tragbaren Datenträger, insbesondere Chipkarte, zum Speichern von Daten in Form von Datensätzen, wobei zur Absicherung des Schreibens und Lesens der Datensätze kryptographische Schlüssel auf dem Datenträger gespeichert sind, sowie ein Verfahren zur Benutzung des Datenträgers.

Im täglichen Leben werden häufig Berechtigungen erworben; Beispiele dafür sind die Berechtigung zur Benutzung von Verkehrsmitteln oder Schwimmbädern. Auf sogenannten Chipkarten, die oft zur Abrechnung von Geldbeträgen verwendet werden, also zum Beispiel eine elektronische Geldbörse enthalten, werden heutzutage auch Berechtigungen in elektronischer Form gespeichert.

Damit stehen Mittel zur Verfügung, die ein umfassendes Abrechnungssystem ermöglichen, in dem mit Hilfe nur einer Chipkarte je Benutzer elektronische Berechtigungen benutzt werden, in dem mit elektronischem Geld bezahlt wird, und andere Transaktionen möglich sind.

Da die sichere Speicherung kryptographischer Schlüssel einen potentiellen Schwachpunkt bezüglich der Sicherheit eines solchen Systems darstellt, möchte man die Verwendbarkeit

...

eines Schlüssels zeitlich so eingrenzen, daß ein Betrug durch Mißbrauch von Schlüsseln aus Zeitgründen erschwert oder gar unmöglich wird. Daher stattet man zum Beispiel in regelmäßigen Abständen neu ausgegebene Chipkarten mit neu gewählten Schlüsseln aus. Die mit den Chipkarten kommunizierenden Sicherheitsmodule in den Endgeräten des Systems, die aus Kostengründen nur zeitweilig mit den diversen Verrechnungsstellen verbunden sind und in der restlichen Zeit selbständig arbeiten, müssen in diesem Fall jedoch über mehrere Generationen von Hauptschlüsseln verfügen, um alle gültigen Karten unterstützen zu können.

Falls kein extrem hoher physikalischer Schutz der Sicherheitsmodule gegeben ist, stellen die langlebigen Hauptschlüssel in den Sicherheitsmodulen selbst einen sicherheitstechnischen Schwachpunkt dar.

Der Erfindung liegt nun die Aufgabe zugrunde, eine Änderung von möglicherweise aus Sicherheitsmodulen ausgespähten Schlüsseln zu ermöglichen, ohne daß damit alle betroffenen Chipkarten ausgetauscht werden müssen. Im Falle eines Diebstahls von Hauptschlüsseln eines Sicherheitsmoduls muß es möglich sein, die entsprechenden Gegenstücke auf allen im Umlauf befindlichen Chipkarten unwirksam zu machen.

Erfindungsgemäß wird diese Aufgabe bei einem tragbaren Datenträger, insbesondere einer Chipkarte, dadurch gelöst, daß eine Reihe von Schlüsseln für den jeweiligen Verwendungszweck auf dem Datenträger gespeichert ist und daß Mittel zur Unbrauchbarmachung von Schlüsseln im Datenträger vorgesehen sind.

Die Schlüssel werden im Normalfall eine bestimmte Zeit lang benutzt und auf Befehl einer Zentrale hin bei der nächsten Verwendung der Chipkarte unbrauchbar gemacht. Gleichzeitig erhalten alle Sicherheitsmodule neue Hauptschlüssel, passend

zu den auf den Chipkarten aktivierten neuen Schlüsseln. Diesen Befehl kann man auch dann geben, wenn der bloße Verdacht eines Betrugsversuchs besteht oder wenn ein Sicherheitsmodul gestohlen wurde. Ein potentieller Betrüger hat damit wenig Zeit, einen Betrug gewinnbringend auszuführen.

Eine erste Weiterbildung des erfindungsgemäßen Datenträgers besteht darin, daß als Mittel zur Unbrauchbarmachung ein Zähler vorgesehen ist, wobei jedem Schlüssel auf dem Datenträger ein Zählerwert zugeordnet ist, daß der Zähler nicht dekrementierbar ist und daß diejenigen Schlüssel unbrauchbar sind, deren Zählerwert kleiner als der Zählerstand ist. Es wird nun auf Befehl einer Zentrale hin bei der nächsten Verwendung der Chipkarte der Zähler inkrementiert und damit ist der bis dahin verwendete Schlüssel ungültig. Sämtliche Sicherheitsmodule werden mit neuen Hauptschlüsseln versorgt. Der Benutzer nimmt von dem Vorgang keine Notiz.

Eine andere Weiterbildung des erfindungsgemäßen Datenträgers sieht Speicherplatz vor zur Aufnahme eines Identifikationsmerkmals des zum Schreiben eines Datensatzes zuletzt verwendeten Schlüssels, beispielsweise des dem Schlüssel zugeordneten Zählerwertes. Bei einer dritten Weiterbildung ist vorgesehen, daß zu jedem Datensatz Speicherplatz vorgesehen ist, worin ein Identifikationsmerkmal desjenigen Schlüssels speicherbar ist, mit dem der Datensatz zuletzt geschrieben wurde. Diese Maßnahmen ergeben eine Kontrollmöglichkeit über die mit der Chipkarte zuletzt verwendeten Schlüssel - entweder für die gesamte Chipkarte oder für einzelne Datensätze, beispielsweise Berechtigungen.

...

Ein erfindungsgemäßer Vorgang, bei dem diese Kontrollmöglichkeit genutzt wird, ist bei dem erfindungsgemäßen Verfahren dadurch verwirklicht, daß vor jeder Benutzung eines Schlüssels zum Schreiben oder Lesen von Daten geprüft wird, ob der Schlüssel älter ist als derjenige, dessen Identifikationsmerkmal auf dem Datenträger gespeichert ist und daß bei positivem Ergebnis dieser Prüfung die Benutzung des Schlüssels abgelehnt wird. So könnte man in dem Fall beispielsweise die betroffene Chipkarte aus dem Verkehr ziehen, da sie offenbar fehlerhaft oder für einen Betrugsversuch mißbraucht worden ist.

Damit der Wechsel von einem alten Schlüssel zu einem neuen reibungslos und automatisch vonstatten geht, ist es vorteilhaft, wie es eine Weiterbildung des erfindungsgemäßen Verfahrens vorsieht, daß vor jeder Benutzung eines Schlüssels zum Schreiben oder Lesen von Daten geprüft wird, ob er neuer ist als derjenige, dessen Identifikationsmerkmal auf dem Datenträger gespeichert ist, daß bei positivem Ergebnis dieser Prüfung das gespeicherte Identifikationsmerkmal durch eines des neueren Schlüssels ersetzt wird und daß alle älteren Schlüssel auf dem Datenträger unbrauchbar gemacht werden. Auf diese Weise werden die Schlüssel auf der Chipkarte nach und nach verbraucht, bis die Gültigkeitsdauer der Chipkarte abgelaufen ist und sie ungültig wird.

Bei einer anderen vorteilhaften Weiterbildung des Verfahrens ist vorgesehen, daß ein zu lesender Datensatz, insbesondere Berechtigungsdatensatz, der mit einem über ein vorgegebenes Maß veralteten Schlüssel geschrieben ist, verworfen wird. Damit läßt sich vermeiden, daß gefälschte Berechtigungen, die mit einem entwendeten älteren Schlüssel erstellt wurden, genutzt werden können.

...

Ausführungsbeispiele der Erfindung sind in der Zeichnung anhand mehrerer Figuren dargestellt und in der nachfolgenden Beschreibung näher erläutert. Es zeigt:

Fig. 1 ein Endgerät als Blockschaltbild sowie eine erfindungsgemäße Chipkarte,

Fig. 2 ein Berechtigungssystem,

Fig. 3 Schlüssel und Zähler erfindungsgemäßer Chipkarten und

Fig. 4 den Vorgang beim Überprüfen eines Schlüssels.

Gleiche Teile sind in den Figuren mit gleichen Bezugszeichen versehen.

Das Blockschaltbild gemäß Fig. 1 umfaßt ein Endgerät 11, das einen Prozessor 12, ein Sicherheitsmodul 13 und ein Karten-Schreib- und Lesegerät 14 enthält. Ferner ist eine Tastatur 15 vorgesehen für Eingaben durch einen Benutzer, falls solche erforderlich sind. Das Sicherheitsmodul 13 ist derart gestaltet, daß Daten- und Programmänderungen sowie ein Auslesen von Programmen und Daten nicht möglich sind. Die einzelnen Baugruppen des Endgerätes 11 sind durch Datenleitungen 16 miteinander verbunden. In das Schreib- und Lesegerät 14 kann eine Chipkarte 17 eingeführt werden.

In dem Berechtigungssystem gemäß Fig. 2, das erfindungsgemäße Chipkarten 17 benutzt, werden die Sicherheitsmodule 13 der Endgeräte 11 von einer physikalisch gesicherten Zentrale 20 aus über ein Telekommunikationsnetz 19 mit Hauptschlüsseln und anderen Informationen versorgt. Diverse Kontrollgeräte 21, 22, die immobile Anwendungen (Schwimmbäder, Telefone) bedienen, sind ebenfalls mit dieser Zentrale 20 verbunden. Andere Kontrollgeräte 23 bedienen

...

mobile Anwendungen, beispielsweise Buslinien 24, und arbeiten autark. Alle Abrechnungen, welche die Endgeräte 11 mit den Chipkarten 17 vornehmen, werden regelmäßig den Verrechnungsstellen 25 (z.B. Banken) mitgeteilt.

Fig. 3 zeigt, wie Schlüssel 32, 33 auf den Chipkarten 17, 17', 17" unbrauchbar werden und wie die Sicherheitsmodule 13 mit neuen Hauptschlüsseln (Masterkey) 31 versorgt werden. Die Hauptschlüssel 31 sind entsprechend ihrer zeitlichen Gültigkeit durchnumeriert. Dazu passende Schlüssel 32, 33 auf den Chipkarten 17, 17', 17" sind ebenfalls mit Nummern versehen, wobei die Schlüssel 33 zu dem mit jeweils gleicher Nummer versehenen Hauptschlüssel 31 passen. Die jeweils durch einen Pfeil symbolisierten Zähler 30, 30', 30" werden beispielsweise jedes halbe Jahr inkrementiert, das heißt bei der ersten Benutzung nach diesem Zeitraum. Alle Schlüssel 32 mit einer kleineren Nummer als der Zählerstand, sind unwirksam und daher in der Figur durchgestrichen. Die Chipkarten 17, 17', 17" haben eine Gültigkeitsdauer von drei Jahren, brauchen also jeweils sechs Schlüssel 32, 33. Jedes Jahr werden neue Chipkarten 17, 17', 17" ausgegeben, so daß die neuen Chipkarten 17, 17', 17" jeweils zwei neue Schlüssel 33 gegenüber der jeweils älteren 17, 17" benötigen. Die Chipkarte 17 ist demnach etwa zwei Jahre alt, Chipkarte 17' ein Jahr und die Chipkarte 17" ist neu. Es sind bei diesem Beispiel ständig drei Generationen G1, G2, G3 von Chipkarten mit insgesamt sechs unwirksamen und wirksamen Schlüsseln 32, 33 im Umlauf.

Wenn die Zentrale 20 einen neuen Hauptschlüssel 31 an die Sicherheitsmodule 13 verteilt, werden nach und nach die Zähler 30, 30', 30" aller Chipkarten 17, 17', 17" inkrementiert, sobald sie mit einem Sicherheitsmodul 13 kommunizieren. Auf diese Weise ist es ausgeschlossen, daß ein Betrüger mit dem Diebstahl eines Sicherheitsmoduls 13 in den Besitz aller Hauptschlüssel 31 kommt, die für die

...

aktuell gültigen Chipkarten 17, 17', 17" vorgehalten werden müssen. Er hat nur die Chance, einen einzigen Hauptschlüssel 31 (mit der Nummer 5) zu erbeuten. Innerhalb des halben Jahres, in dem der erbeutete Hauptschlüssel 31 gültig ist läßt sich ein Betrug jedoch kaum gewinnbringend ausführen.

Das Flußdiagramm gemäß Fig. 4 zeigt die Anwendung eines Schlüssels, wobei nach einem Start bei 40 bei 41 der neue Schlüssel KN und bei 42 der alte Schlüssel KO gelesen werden. Bei 43 wird geprüft, ob der neue Schlüssel KN neuer als oder gleich alt wie der bis dahin verwendete alte Schlüssel KO ist. Ist dies nicht der Fall, wird die Operation bei 44 abgebrochen. Anderenfalls wird bei 45 geprüft, ob der neue Schlüssel KN neuer als der alte Schlüssel KO ist. Zutreffendenfalls wird im Schritt 46 KO auf KN gesetzt. In beiden Fällen wird bei 47 die Berechtigung A freigegeben.

...

Ansprüche

1. Tragbarer Datenträger, insbesondere Chipkarte, zum Speichern von Daten in Form von Datensätzen, wobei zur Absicherung des Schreibens und Lesens der Datensätze kryptographische Schlüssel (32, 33) auf dem Datenträger (7) gespeichert sind, dadurch gekennzeichnet, daß eine Reihe von Schlüsseln (32, 33) für den jeweiligen Verwendungszweck auf dem Datenträger (7) gespeichert ist und daß Mittel (30) zur Unbrauchbarmachung von Schlüsseln (32, 33) im Datenträger (7) vorgesehen sind.

2. Datenträger nach Anspruch 1, dadurch gekennzeichnet, daß als Mittel zur Unbrauchbarmachung ein Zähler (30) vorgesehen ist, wobei jedem Schlüssel (32, 33) auf dem Datenträger ein Zählerwert zugeordnet ist, daß der Zähler (30) nicht dekrementierbar ist und daß diejenigen Schlüssel (32) unbrauchbar sind, deren Zählerwert kleiner als der Zählerstand ist.

3. Datenträger nach einem der vorhergehenden Ansprüche, gekennzeichnet durch Speicherplatz zur Aufnahme eines Identifikationsmerkmals (42) des zum Schreiben eines Datensatzes zuletzt verwendeten Schlüssels (33), beispielsweise des dem Schlüssel (33) zugeordneten Zählerwertes.

...

4. Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß in jedem Datensatz, insbesondere Berechtigungsdatensatz, Speicherplatz vorgesehen ist, worin ein Identifikationsmerkmal (42) desjenigen Schlüssels (33) speicherbar ist, mit dem der Datensatz zuletzt geschrieben wurde.

5. Verfahren zur Benutzung eines Datenträgers nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß vor jeder Benutzung eines Schlüssels (33) zum Schreiben oder Lesen von Daten geprüft wird, ob der Schlüssel (33) älter ist als derjenige, dessen Identifikationsmerkmal (42) auf dem Datenträger gespeichert ist und daß bei positivem Ergebnis dieser Prüfung die Benutzung des Schlüssels (33) abgelehnt wird.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß vor jeder Benutzung eines Schlüssels (33) zum Schreiben oder Lesen von Daten geprüft wird, ob er neuer ist als derjenige, dessen Identifikationsmerkmal (42) auf dem Datenträger gespeichert ist, daß bei positivem Ergebnis dieser Prüfung das gespeicherte Identifikationsmerkmal (42) durch eines (40) des neueren Schlüssels ersetzt wird und daß alle älteren Schlüssel (32) auf dem Datenträger unbrauchbar gemacht werden.

7. Verfahren nach einem der Ansprüche 5 oder 6, dadurch gekennzeichnet, daß ein zu lesender Datensatz, insbesondere Berechtigungsdatensatz, der mit einem über ein vorgegebenes Maß veralteten Schlüssel geschrieben ist, verworfen wird und insbesondere die Berechtigung verworfen wird.

...

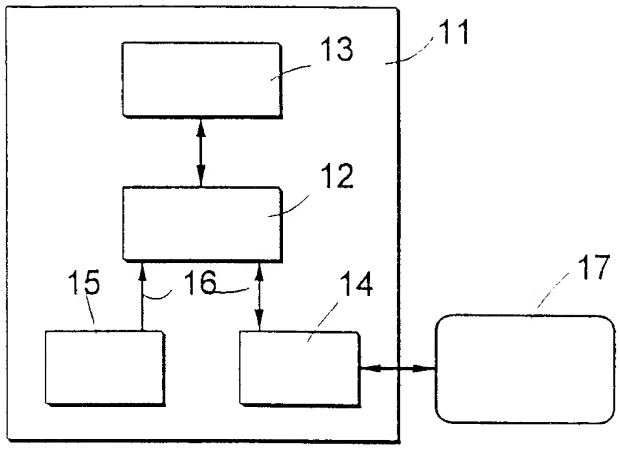

13
11
12
15
16
14
17

Fig.1

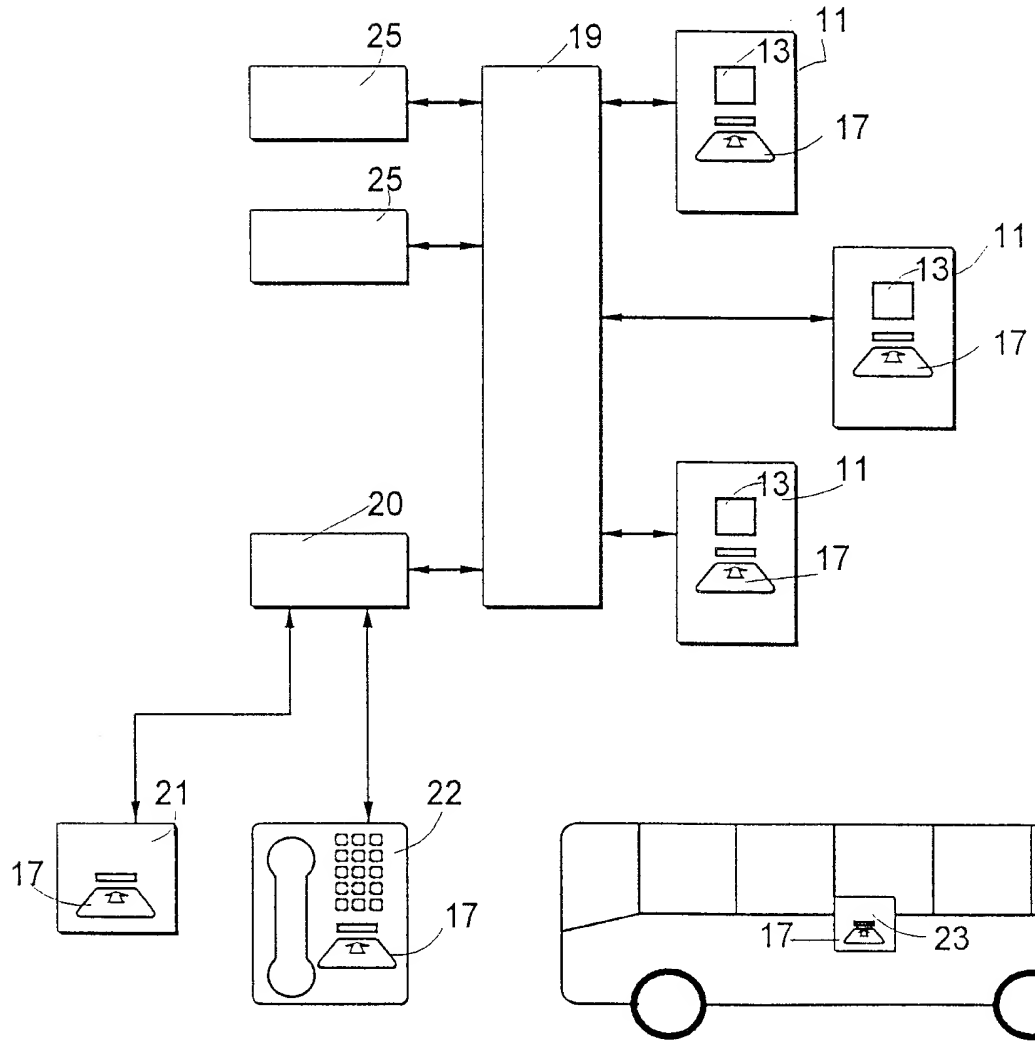

25
19
11
13
17
25
11
13
17
20
11
13
17
21
22
17
17
24
17
23

Fig.2

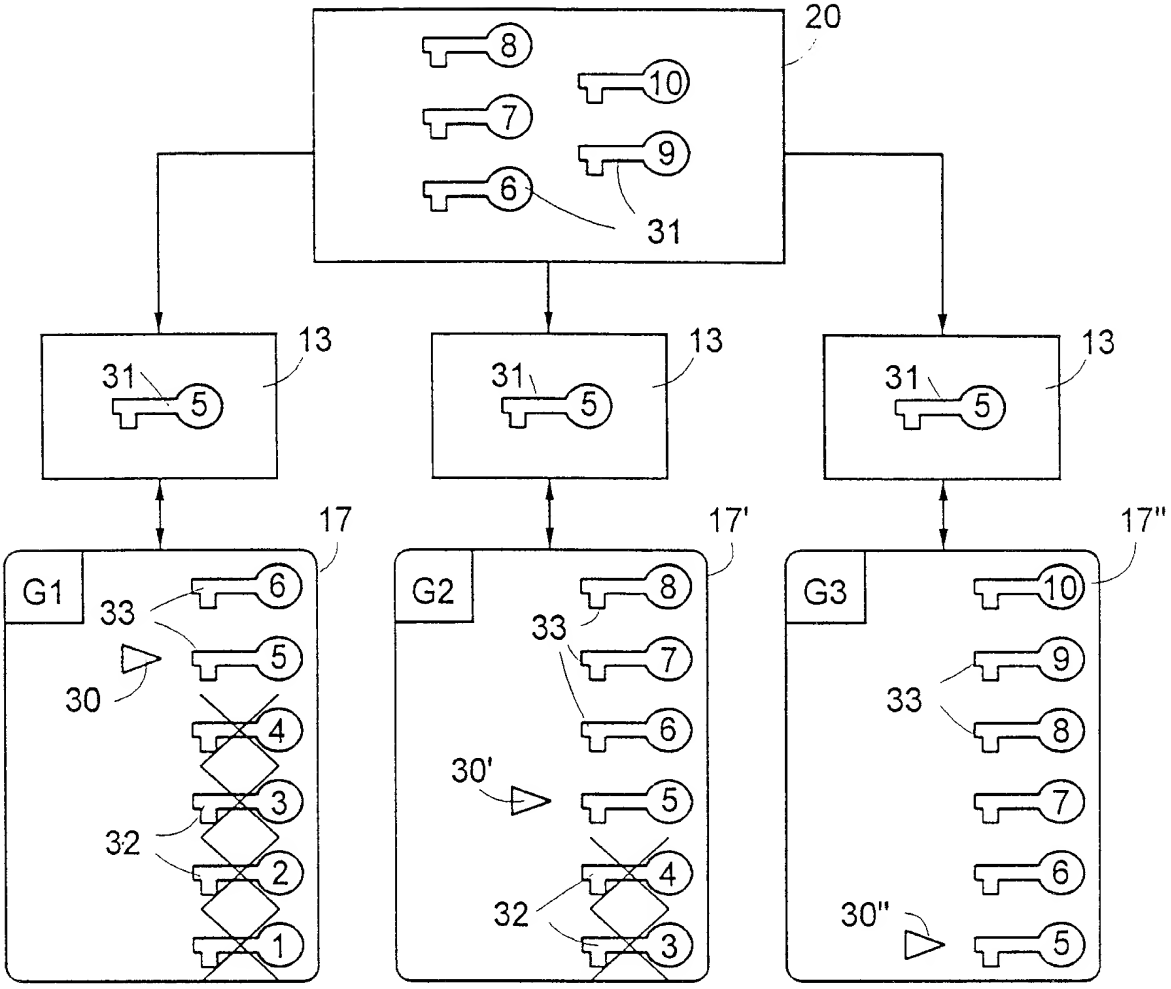

20
8
10
7
9
6
31
13
31
5
13
31
5
13
31
5
17
17'
17"
G1
G2
G3
33
30
30'
30"
32
6
5
4
3
2
1
8
7
6
5
4
3
10
9
8
7
6
5

Fig.3

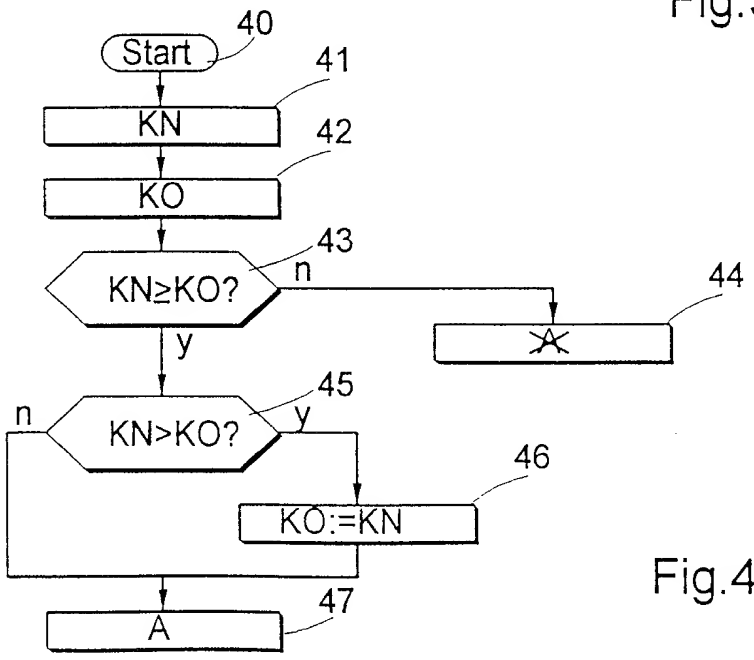

Start
40
41
KN
42
KO
43
KN≥KO?
n
44
y
45
n
KN>KO?
y
46
KO:=KN
47
A

Fig.4